BUNDESREPUBLIK DEUTSCHLAND

09/673658

EP99/2848

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

REC'D 20 JUL 1999
WIPO PCT

Bescheinigung

Die Giesecke & Devrient GmbH in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zur Authentisierung einer Chipkarte innerhalb eines Nachrichtenübertragungs-Netzwerks"

am 7. Mai 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole H 04 L und G 07 F der Internationalen Patentklassifikation erhalten.

München, den 2. Juni 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Seiler

Aktenzeichen: 198 20 422.1

A 9161
06.90
11/98

gewählte „Zufallszahlen" nach dem standardisierten Protokoll an die SIM-Karte übermittelt werden und daraus, nach mehrfachen Authentisierungsversuchen, der Geheimschlüssel der Chipkarte ermittelt wird. Ist zusätzlich der Algorithmus der Karte bekannt, können nach Ermittlung des geheimen Schlüssels wesentliche Funktionselemente der Karte simuliert bzw. dupliziert werden.

Es ist deshalb Aufgabe der Erfindung, ein sicheres Verfahren zur Authentisierung einer Chipkarte in einem Nachrichtensystem anzugeben, bei dem, wie beispielsweise im GSM-Netz üblich, eine Rückmeldung über das Authentisierungsergebnis an die teilnehmende Chipkarte nicht erfolgt.

Diese Aufgabe wird gemäß der Erfindung ausgehend von den Merkmalen des Oberbegriffs des Anspruchs 1 durch die kennzeichnenden Merkmale des Anspruchs 1 gelöst.

Vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

Die Erfindung sieht vor, zur Bildung der Authentisierungsnachricht sowohl aus dem geheimen Schlüssel als auch aus der vom Netzwerk übertragenen Zufallszahl jeweils wenigstens zwei Teile zu bilden, wobei einer der Teile der übertragenen Zufallszahl und einer oder mehrere Teile des geheimen Schlüssels mittels eines ein- oder mehrstufigen, vorzugsweise symmetrischen Berechnungsalgorithmus verschlüsselt werden. Zur Ausgabe einer Authentisierungsnachricht wird ein auswählbarer Teil des nach dem Authentisierungsalgorithmus berechneten Ergebnisses an das Netzwerk übertragen.

Eine vorteilhafte Ausgestaltung der Erfindung sieht vor, daß in der gleichen Art und Weise auch der Kanalkodierungsschlüssel erzeugt wird, d.h. auch dort ist, beispielsweise bei einer Zweiteilung des Schlüssels und der Zufallszahl vorgesehen, daß entweder der erste oder der zweite Teil der übertragenen Zufallszahl mit dem ersten und/oder zweiten Teil des geheimen Schlüssels mit einem ein- oder mehrstufigen Algorithmus verknüpft werden, um einen Kanalkodierungsschlüssel zu erhalten. Vorzugsweise werden für die Bildung der Authentisierungsnachricht und des Kanalkodierungsschlüssels jeweils verschiedene Teile der vom Netzwerk erhaltenen Zufallszahl verwendet.

Eine weitere vorteilhafte Ausgestaltung der Erfindung sieht vor, daß der in der Karte abgelegte geheime Schlüssel sowie die Zufallszahl, welche vom Netzwerk an die Karte gesendet wird, in gleich lange Teile aufgeteilt werden. Damit kann in beiden Fällen der gleiche Berechnungsalgorithmus verwendet werden. Die Aufteilung der Zufallszahl bzw. des geheimen Schlüssels kann in der Weise erfolgen, daß eine einfache Teilung "in der Mitte" erfolgt oder sich überlappende Teilbereiche entstehen. Ebenso ist eine Teilung denkbar, in der die Summe der einzelnen Teile kleiner ist als die Bit-Länge der Zufallszahl bzw. des geheimen Schlüssels. Gemäß einer weiteren Variante können nach einem vorbestimmten Muster oder pseudozufällig jeweils eine vorgegebene Anzahl von Bits der Zufallszahl bzw. des geheimen Schlüssels zu jeweils einem Schlüssel- bzw. Zufallszahlenteil zusammengefaßt werden.

Als weitere vorteilhafte Ausgestaltung der Erfindung können als Berechnungsalgorithmen zur Authentisierung sowie zur Kanalkodierung DES-Algorithmen verwendet werden.

Eine andere vorteilhafte Variante der Erfindung sieht vor, daß zur Berechnung der Authentifizierungsparameter und der Kanalkodierungsschlüssel der vorzugsweise einstufige IDEA-Algorithmus verwendet wird.

Alternativ können zur Berechnung der Authentifizierungsparameter und der Kanalkodierungsschlüssel Komprimierungsalgorithmen, vorzugsweise kryptografische Komprimierungsalgorithmen verwendet werden, deren Ausgabewerte eine geringere Länge als die Eingabeparameter aufweisen.

Zur Erhöhung der Sicherheit ist es vorteilhaft, einen mindestens zweistufigen Berechnungsalgorithmus zu verwenden, wobei sich ein Triple-DES-Algorithmus als besonders sicher erweist. Bei diesem Algorithmus wird zunächst mit einem ersten Teil des Schlüssels und einem Teil der Zufallszahl verschlüsselt, anschließend wird eine Entschlüsselung des Ergebnisses mit dem zweiten Teil des Schlüssels vorgenommen, um schließlich wieder mit dem ersten Teil des Schlüssels eine weitere Berechnung auszuführen. Bei der letzten Verschlüsselung mit dem ersten Teil des Schlüssels kann in vorteilhafter Weise, insbesondere bei einer Schlüsselaufteilung in drei Schlüsselteile, ein neuer, dritter Schlüssel verwendet werden.

Eine weitere vorteilhafte Ausgestaltung der Erfindung ergibt sich, wenn die Auswahl des ersten oder zweiten Teils der Zufallszahl für die Authentisierung bzw. die Berechnung der Kanalkodierung im Wechsel erfolgt, wobei dieser Wechsel zufällig bzw. pseudozufällig ausgeführt wird und die Auswahl in der Karte und im Netzwerk auf die gleiche Weise erfolgt.

Im folgenden wird die Erfindung an Hand der Figuren 1 bis 3 näher beschrieben.

Fig. 1 zeigt den Ablauf der kryptographischen Funktionen des SIM im GSM-Netz.

Fig. 2 zeigt ein Blockschaltbild der Triple DES-Verschlüsselung.

Fig. 3 zeigt Beispiele für die Aufteilung des geheimen Schlüssels bzw. der Zufallszahl

Bei dem in Fig. 1 dargestellten Ablauf wird vorausgesetzt, daß der übliche, vorhergehende Vorgang der PIN-Verifizierung abgeschlossen ist. Im Anschluß daran wird von der mobilen Einheit, in der sich die Karte SIM befindet, eine Nachricht an das Netzwerk gesendet, welche eine IMSI- (international mobile subscriber identity) Information bzw. eine TMSI- (temporary mobile subscriber identity) Information enthält. Aus der IMSI bzw. TMSI wird im Netzwerk nach einer vorgegebenen Funktion oder mittels einer Tabelle ein geheimer Schlüssel K_i bestimmt. Derselbe Schlüssel ist auch in der Chipkarte SIM in einem nicht zugänglichen Speicherbereich abgelegt. Der geheime Schlüssel wird für die spätere Verifizierung des Authentisierungsvorganges benötigt.

Das Netzwerk initiiert sodann den Authentisierungsvorgang, indem es eine Zufallszahl RAND berechnet und diese über die Luftschnittstelle an die Chipkarte SIM überträgt.

In der Chipkarte wird daraufhin mittels eines Authentisierungsalgorithmus aus dem geheimen Schlüssel K_i und der Zufallszahl RAND ein Authentisierungsparameter SRES gebildet, der über die Luftschnittstelle wiederum an das Netzwerk übertragen wird. Erfindungsgemäß werden hierbei aus der Zufallszahl RAND mindestens zwei Zufallszahlen $RAND_1$ und $RAND_2$ ab-

geleitet. Die Zufallszahlen $RAND_1$ und $RAND_2$ können durch Teilung oder eine Auswahl aus der Zufallszahl RAND bzw. durch einen Berechnungsalgorithmus gewonnen werden.

Die Authentisierung erfolgt im Ausführungsbeispiel nach Fig. 1 mit einem zweistufigen Algorithmus. Dabei wird, wie in Fig. 1 angedeutet, zunächst der erste Teil der Zufallszahl $RAND_1$ mit einem ersten Teil K_1 des ebenfalls in zwei Teile aufgeteilten Schlüssels K_i verschlüsselt. Das Ergebnis dieser ersten Stufe wird anschließend in einer zweiten Stufe mit dem zweiten Teil des Schlüssels K_2 verschlüsselt. Selbstverständlich kann zur Berechnung mit dem Authentisierungsalgorithmus zunächst auch der zweite Teil der Zufallszahl $RAND_2$ verwendet und die Reihenfolge der Verwendung der ersten und zweiten Schlüsselteile K_1 und K_2 verändert werden.

Im Netzwerk wird währenddessen auf dieselbe Weise wie in der Karte mittels des Authentisierungsalgorithmus und der Zufallszahl RAND ($RAND_1$, $RAND_2$) sowie dem geheimen Schlüssel K_i (K_1, K_2) ebenfalls ein Authentisierungsparameter SRES' gebildet. Der Parameter SRES' wird im Netzwerk sodann mit dem von der Karte erhaltenen Authentisierungsparameter SRES verglichen. Stimmen beide Authentisierungsparameter SRES' und SRES überein, wird der Authentisierungsvorgang erfolgreich abgeschlossen. Stimmen die Authentisierungsparameter nicht überein, gilt die Karte des Teilnehmers als nicht authentisiert. Es sei an dieser Stelle angemerkt, daß zur Bildung von SRES bzw. SRES' auch nur Teile aus dem durch die Verschlüsselung erhaltenen Ergebnisses verwendet werden können.

In der gleichen Weise wie die Erzeugung der Authentisierungsparameter erfolgt in der Karte und im Netzwerk die Generierung eines Schlüssels K_c für Kanalkodierung für die Daten- und Sprachübertragung. Vorzugsweise

Die Figur 3a zeigt einen Schlüssel K_i bzw. eine Zufallszahl RAND mit einer Länge von 128 bit.

In der Figur 3b ist eine Aufteilung in zwei gleiche Teile K_1 und K_2 ($RAND_1$, $RAND_2$) dargestellt, wobei die Aufteilung mittig erfolgt. Teil 1 enthält bit 1 bis bit 64, Teil 2 enthält bit 65 bis bit 128. In Figur 3c ist eine überlappende Aufteilung angegeben und in der Figur 3d ist eine Aufteilung dargestellt, bei der jeweils die ungeradzahligen bits dem Teil 1 und die geradzahligen bits dem Teil 2 zugeordnet sind. Figur 3e zeigt schließlich eine Aufteilung, bei der die Summe der Binärstellen der Teile 1 und 2 kleiner ist als die Binärstellen des Ausgangsschlüssels bzw. der Ausgangszufallszahl.

Patentansprüche

1. Verfahren zur Authentisierung einer Chipkarte (SIM) in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM-Netzwerk, bei dem in einer Chipkarte (SIM) ein Algorithmus sowie ein geheimer Schlüssel gespeichert sind, wobei zur Authentisierung
- zunächst vom Netzwerk oder einer Netzwerkkomponente eine Zufallszahl (RAND) an die Chipkarte übertragen wird,
- in der Chipkarte daraus mittels des Algorithmus und des geheimen Schlüssels (K_i)ein Antwortsignal (SRES) erzeugt und an das Netzwerk bzw. die Netzwerkkomponente übermittelt wird,
dadurch gekennzeichnet, daß
- zur Bildung eines Authentisierungsparameters der geheime Schlüssel (K_i) sowie die Zufallszahl (RAND) in jeweils wenigstens zwei Teile (K_1, K_2; $RAND_1$, $RAND_2$) aufgeteilt werden,
- einer der Teile ($RAND_1$, $RAND_2$) der übertragenen Zufallszahl (RAND) mit Hilfe eines oder mehrerer Teile (K_1, K_2) des geheimen Schlüssels (K_i) mittels eines ein- oder mehrstufigen, vorzugsweise symmetrischen Algorithmus verschlüsselt werden, und
- eine vorgegebene Anzahl von Bits aus dem Verschlüsselungsergebnis ausgewählt und als Signalantwort (SRES) an das Netzwerk übertragen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der geheime Schlüssel (Ki) und/oder die Zufallszahl (RAND) in zwei Teile aufgeteilt werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß ein Teil der übertragenen Zufallszahl (RAND) sowie ein und/oder weitere Teile des geheimen Schlüssels (Ki) zur Berechnung eines Kanalko-

dierungsschlüssels (K_c) mittels eines ein- oder mehrstufigen Algorithmus verwendet werden, wobei zumindest ein Teil des Berechnungsergebnisses als Kanalkodierungsschlüssel (K_c) verwendet wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der Schlüssel (K_i) sowie die Zufallszahl (RAND) in zwei gleich lange Teile (K_1, K_2/$RAND_1$, $RAND_2$) aufgeteilt werden.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß zur Berechnung der Authentifizierungsparameter (SRES, SRES´) und/oder des Kanalkodierungsschlüssels (K_c) DES-Algorithmen verwendet werden.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß zur Berechnung der Authentisierungsparameter (SRES, SRES´) und/oder des Kanalkodierungsschlüssels (K_c) der, vorzugsweise einstufige, IDEA-Algorithmus verwendet wird.

7. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß zur Berechnung der Authentisierungsparameter (SRES, SRES´) und/oder des Kanalkodierungsschlüssels (K_c) ein Komprimierungsalgorithmus verwendet wird, dessen Ausgabewert eine geringere Länge als der Eingabeparameter aufweist.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß die Berechnung in einem mindestens zweistufigen Algorithmus erfolgt.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß als Verschlüsselungsalgorithmus ein Triple-DES-Algorithmus verwendet wird, bei dem zunächst mit dem ersten Teil (K_1) des Schlüssels (K_i) verschlüsselt, anschließend mit dem zweiten Teil (K_2) des Schlüssels (K_i) entschlüsselt und darauf wieder mit dem ersten Teil (K_1) oder einem dritten Teil des Schlüssels (K_i) verschlüsselt wird.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß eine Auswahl des ersten oder zweiten Teils der Zufallszahl (RAND) im zufälligen oder pseudozufälligen Wechsel in der Karte und im Netzwerk in gleicher Weise erfolgt.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Authentisierung einer Chipkarte (SIM) in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM-Netzwerk, bei dem in einer Chipkarte (SIM) ein gegebenenfalls geheimer Algorithmus sowie ein geheimer Schlüssel gespeichert ist, wobei zur Authentisierung zunächst vom Netzwerk oder einer Netzwerkkomponente eine Zufallszahl an die Chipkarte übertragen wird, in der Chipkarte mittels des Algorithmus, der Zufallszahl und des geheimen Schlüssels ein Antwortsignal erzeugt wird, das an das Netzwerk bzw. die Netzwerkkomponente übermittelt wird, um dort die Authentizität der Karte zu überprüfen. Gemäß der Erfindung wird zur Bildung der Authentisierungsnachricht sowohl der geheime Schlüssel als auch die vom Netzwerk übertragene Zufallszahl in jeweils wenigstens zwei Teile aufgeteilt, wobei ein Teil der übertragenen Zufallszahl und ein oder mehrere Teile des geheimen Schlüssels mittels eines ein- oder mehrstufigen, vorzugsweise symmetrischen Berechnungsalgorithmus verschlüsselt werden. Zur Ausgabe einer Authentisierungsantwort wird ein auswählbarer Teil des Verschlüsselungsergebnisses an das Netzwerk übertragen.

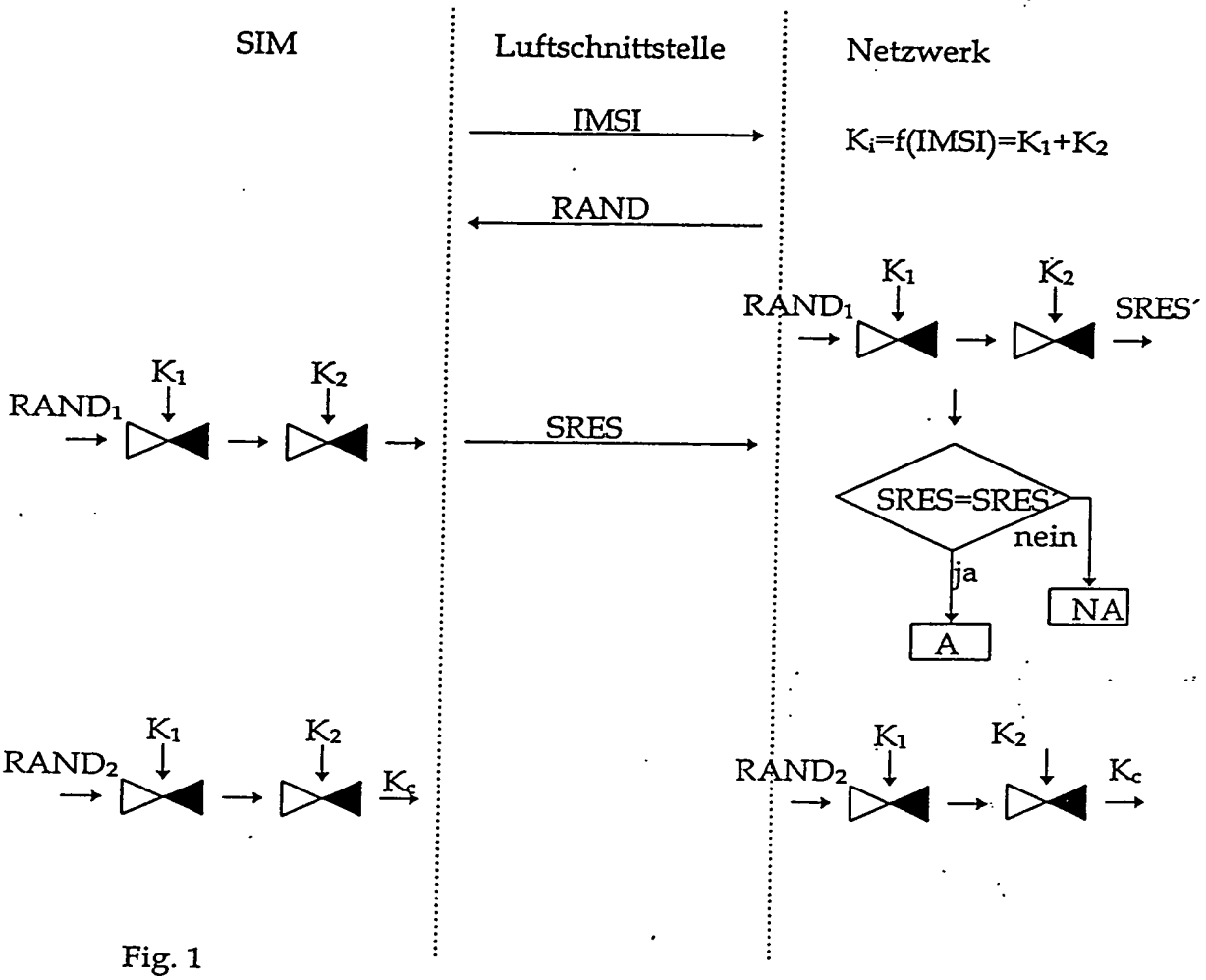
SIM
Luftschnittstelle
Netzwerk
IMSI
$K_i=f(IMSI)=K_1+K_2$
RAND
$RAND_1$
K_1
K_2
SRES´
SRES
SRES=SRES´
nein
ja
NA
A
$RAND_2$
K_c

Fig. 1

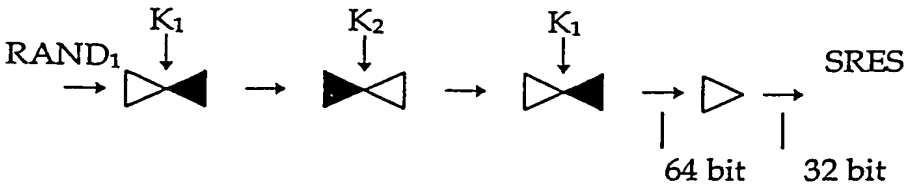
$RAND_1$
K_1
K_2
K_1
SRES
64 bit
32 bit

Fig. 2

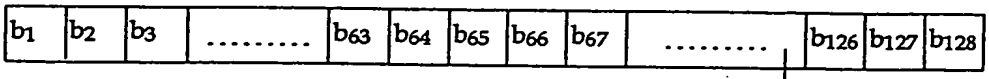

Fig. 3a

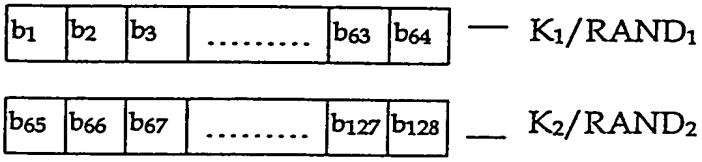

Fig. 3b

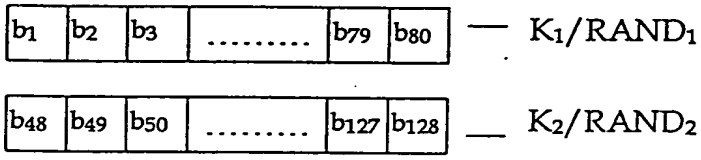

Fig. 3c

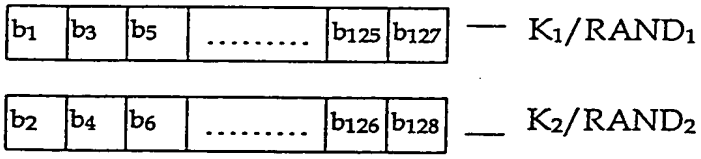

Fig. 3d

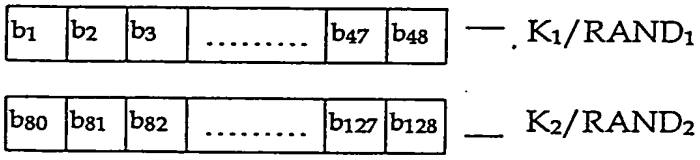

Fig. 3e